Hosting and Application Development Strategy

Digital Delivery Unit
June 2020

BRITISH COLUMBIA

Ministry of
Citizens' Services

OCIO

Office of the
Chief Information Officer

Hosting and Application Development Strategy

June 2020

Contents

Executive Summary

Governments around the world are embracing digital tools to better serve citizens and empower their workforce. Technology has created new opportunities, as well as new expectations, for how governments provide services. The Government of British Columbia is actively investing in digital government to improve the services that people count on.

Government now has an opportunity to leverage new technologies to modernize its approach to hosting the applications that support digital services. New cloud-based technologies offer opportunities to deliver value. **This Hosting and Application Development Strategy offers a vision and approach for modernizing government's efforts to provide excellent digital services to British Columbians by using best practices in hosting and application development.**

The vision offered here is expected to improve the efficiency, quality and sustainability of government's digital assets. These assets relate to information management (IM) and information technology (IT), such as payment and identity systems. Ultimately, the strategy aims to help government deliver and operate information systems that support the services British Columbians rely on.

Background

The last time the B.C. government made a significant change to its approach to IT was in 2009. It applied industry best practices at that time. It consolidated and outsourced staffing and managing B.C. government data centres. It successfully shifted the data centres geographically away from earthquake and flood zones and managed them using a centralized team of IT specialists.

In 2024, the Hosting Data Centre and Managed Services Agreements will both be expiring. By 2025, Gartner predicts 80% of traditional data centres will be closed. While government will certainly still require on-premise services in 2024, government must act now to ensure good stewardship of government assets that support services for the people and businesses of British Columbia.

Vision and principles

This strategy is intended to give clear direction to government on the future of IT. It focuses on hosting and application development for business solutions, and thereby sets the foundations for modern service delivery for the next 10 years and beyond.

This strategy is one element of a broader Hosting and Application Development Framework. The strategy describes the challenges in government's current IT service delivery model, as well as opportunities for improvement, and proposes strategic steps to capitalize on the opportunities.

The Hosting and Application Development Strategy articulates three key principles:

1. **Strengthen technical capabilities, at the centre and in the ministries**
   Government will: support empowered, distributed communities of technologists; automate IT provisioning through routinized, scriptable and repeatable processes; and formalize and adopt robust architectural standards.

2. **Avoid being "too big to fail"**
   Government will: more effectively leverage procurements across government; prioritize independent professional services that add the greatest value; effectively orchestrate hosting services to maximize network performance and data portability; and act as an informed consumer of increasingly sophisticated hosting services.

3. **Adopt fit-for-purpose solutions and internet-era approaches**
   Government will collaborate with partners and vendors to maximize the return on investment by: adopting the highest-level services that meet business needs, including by minimizing unnecessary customization; adopting best practices in software development when custom application development is necessary; and convening integrated, cross-functional teams in developing applications.

These principles represent a significant investment in iteratively improving the Government of British Columbia's technology capacity. They support a vision of technology across government that focuses on:

1. Working better together;
2. Technical diligence;
3. Service model fit;
4. Cost optimization;
5. Collaboration over contract negotiation;
6. Sustainable application portfolio; and
7. Keeping pace in the security race.

This strategy has resulted from a collaborative effort between the Government of British Columbia's Office of the Chief Information Officer (OCIO) and ministries. It has also benefited from feedback generously provided by the public by virtue of practicing the OCIO principle of working in the open.

1. *Introduction*

The Government of British Columbia is always looking to modernize its business processes, models, and technologies. By improving digital tools and services for people, businesses and public servants, we aim to enhance our service delivery and make government more effective and efficient.

The Digital Framework is our plan to embrace best practices in digital government. Using the framework as our guide, the OCIO is leading modernization efforts and working collaboratively across government.

Under the Core Policy and Procedures Manual (CPPM, Chapter 12), the OCIO is responsible for providing strategic direction for government on IT/IM. Our technology infrastructure is a key enabler supporting business transformation. This strategy offers a vision for the future of IT and principles that can enable a progressive transition towards the vision.

Background

Over 1,600 applications run in our data centres, many of which serve similar business purposes. These applications, some of which are 30 years old, were built for specific needs. As business needs have evolved, older applications have become expensive to run, difficult to maintain, and complicated to manage due to increased security and privacy risks. They also pose unique challenges in the face of changing business processes and services.

We have identified the following challenges that have led to and continue to contribute to our current state:

- Delivery silos that prevent collaboration and integration between units;
- Technology drift, where legacy systems introduce risk and are slow to adapt;
- A gap in the service model that falls short of meeting ministry needs;
- A pit of costs connected with a delivery model that lacks transparency and is expensive to maintain;
- Contract challenges related to existing procurement processes, which restrict flexibility and reuse of products and services.
- Unsustainable application growth where new applications are consistently built without decommissioning old infrastructure; and
- Falling behind in the security marathon and striving to keep pace with ever-evolving industry best practices.

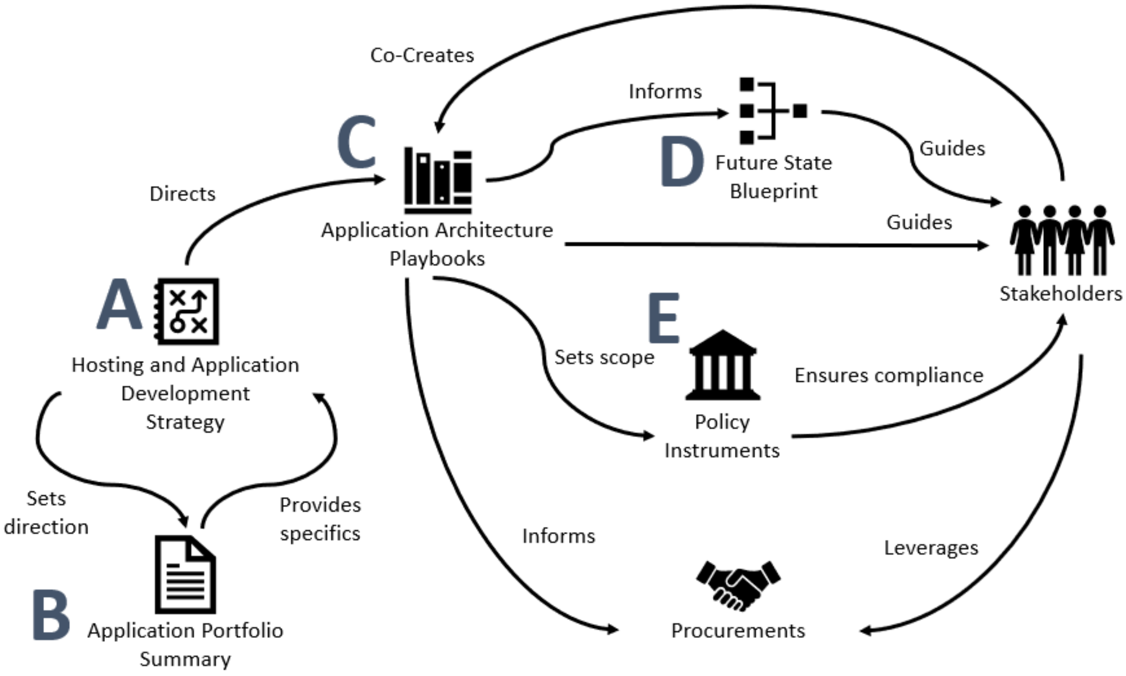
The Hosting and Application Development Framework (the Framework) will address these challenges by setting clear direction, offering modern tools, and assisting ministries in making decisions around modernizing and replacing these applications. This work will occur over the next three years, to 2024, to align with the end of the current hosting contracts.

Context of this strategy

This Hosting and Application Development Strategy is part of the broader Hosting and Application Development Framework. The overall Framework is ambitious in scope. It includes efforts to support the delivery of solutions for people, businesses, and public servants, as well as streamlining service delivery within the public sector by adopting modern tools. The Framework will improve the processes and strategies for enterprise IT investments as well as creating the appropriate policies to guide good technology decisions.

There are five planned workstreams for the Framework:

A. Hosting and Application Development Strategy (this document)
B. Application Portfolio Summary
C. Playbook for Modern Application Architecture
D. Future State Blueprint
E. Policy Instruments



The Framework will allow us to be more collaborative and responsive to end-user expectations. It will document the current state, provide a future state vision, and map an approach to achieve this vision.

Framework deliverables will be developed in the open and in collaboration with stakeholders including Ministry Chief Information Officers (MCIOs), the Technology Innovation Forum (a group of cross-government leaders interested in advancing digital and technology solutions), and other cross-ministry partners, executive sponsors, and the public. The audience for this strategy consists of Assistant Deputy Ministers, MCIOs, and project delivery leads.

2. *Opportunities for modern hosting and application development*

Many private and public sector organizations struggle to keep up with changing service expectations. Technology can be both an enabler and a barrier to delivering excellent services that meet people's expectations. Government service delivery can sometimes make people feel underwhelmed.

Examples of underwhelming service delivery include:

- Being required to fax a document rather than submit it online;
- Taking time off work to receive a service that could be automated; and
- Waiting in a phone queue rather than texting or instant messaging.

The B.C. government is committed to providing quality services that are efficient and sustainable. Negative service experiences matter because our customers cannot take their business elsewhere. Research shows that customer experience affects the public's confidence and trust in their governments (McKinsey, 2019).

Problems we are seeking to solve

To improve service delivery, government must become digital on the inside. Technology is essential to the functioning of the public service, but the digital tools available to public servants at the workplace are sometimes inferior to what they can access at home. This affects people's confidence in government and can also demoralize staff due to lost productivity.

This strategy seeks to address the following challenges:

Client ministries are seeking modern services from OCIO	Ministries and partners would benefit from a clear government-wide strategy	Modern hosting would support and accelerate the digital framework
•Through recent user research on cloud, ministries expressed interest in an improved OCIO service model for hosting •Particular interest in clear policies and guidelines, enterprise-level agreements, predictable timelines and easy-to-access solutions •Ministries are seeking alternatives to the current model but are unsure of options and burdened with the current state	•Approximately 1,600 applications in the data centres •Opportunities to provide pathways to modernize and improve government-wide approaches and tools for hosting, managing applications and providing services •Lift-and-shift strategies to cloud have not generally been successful. Government needs a better approach	•Work aligns closely with our commitment to being digital inside •Consistent with our Digital Principles and expected updates to Chapter 12 •Gartner predicts that by 2025, 80% of enterprises will shut down their traditional data centers •Potential opportunities to leverage modern hosting to improve costing and elasticity

The digital era requires a fundamental shift in mindsets and a change in how government procures, builds, and manages technology. The B.C. public service has an opportunity to become a leader in digital government, providing modern tools and services to citizens and public servants alike.

To become digital on the inside, government needs take decisive action, including to:

- Support leaders in taking a visionary approach to creating services;
- Attract and retain digital talent; and
- Ensure staff have the tools and resources required to deliver digital services.

This Hosting and Application Development Strategy offers a vision and approach for modernizing government's efforts to provide excellent digital services to British Columbians by using best practices in hosting and application development.

Current application landscape

The B.C. government's last significant change to its hosting and data centre approach was in 2009. It consolidated and outsourced staffing and managing B.C. government data centres. It successfully shifted the data centres geographically away from earthquake and flood zones and managed them using a centralized team of IT specialists. There was a mass migration of physical to virtual servers. This was largely done through a "lift and shift" approach without addressing the underlying technologies or business processes.

What we know about government's 1,600+ applications:

- Approximately 70% of applications are custom built by ministries
- Roughly 70% are internal facing only
- User intensity:
  - 59% have less than 100 users;
  - 24% have approximately 100-999 users;
  - 17% have more than 1,000 users
- 74% are on virtual servers versus 26% on physical servers

Further detail will be included in the Application Portfolio Summary. This detail is expected to include a breakdown of applications by ministry, hosting and maintenance costs, and overall technology baseline.

Trends in hosting solutions

In the past, government purchased or developed large software systems. This approach required a large investment in technology infrastructure. The resulting contracts often led to expensive, multi-year vendor lock-in and isolation of specialized knowledge. For government, vendor lock-in has meant being heavily dependent on individual vendors, which fuels costs, prevents competition, and stifles innovation.

Such investments often reinforced ministries' siloed approaches to products and services. Siloed units prioritized their own business needs, which often resulted in unique IT investments, standards and implementations. This outcome further prevented collaboration, information exchange, and adoption of common approaches.

Whereas the past consisted of large, on-premise solutions, the trend is now towards technology as a utility or a commodity. This means that it is easier to move between service providers and to scale up or down as required. Similarly, large single-purpose monoliths are being replaced with smaller, reusable components. The Framework will accomplish this by making modern tools and approaches the default.

Alignment with other initiatives

The Core Policy and Procedures Manual Chapter 12 outlines how the OCIO is responsible for taking a leadership role in the “design, development, delivery, maintenance, evaluation and continuous improvement of enterprise solutions” (12.3.4). Accordingly, the Government Chief Information Officer (GCIO) announced the Hosting and Application Development Framework in December 2019. The goal of the framework is to provide a path to modernize and improve government-wide approaches and tools for hosting and managing applications. This means fostering a culture that is responsive to citizen and ministry needs.

Guidance for the Framework draws on service design approaches from the Digital Framework and the Ministry of Citizens’ Services (CITZ) Service Transformation Initiative as well as the government’s commitment to more versatile procurement.

The Framework is being developed in alignment with key policies, principles, and practices across the B.C. government, including:

- OCIO Principles of Work
- B.C. Government Procurement Strategy
- Digital Framework
- Digital Principles (draft v.0.2)
- Core Policy and Procedures Manual - Chapter 12 (draft v.0.2)
- Service Design Playbook

These foundational documents establish how government IT is being transformed. Additionally, these initiatives provide core elements supporting the strategic intent to promote the B.C. economy where “local, small and medium-sized companies can do business with government more efficiently while ensuring public funds are spent wisely” (CITZ 2020 Minister's Mandate Letter).

The work is further informed by the B.C. government’s commitments to diversity and inclusion. These commitments include the 2019 *Declaration on the Rights of Indigenous Peoples Act*, advancing reconciliation, as well as commitments to equality and diversity, including through Gender-Based Analysis Plus (GBA+). As we develop the Framework that will drive major changes in IT service delivery across government, it is important that these activities are underpinned by reconciliation, diversity and inclusion.

3. Where are we going

Current state

Through stakeholder engagement, as well as an analysis of the government's current IT service delivery model, seven key challenges have been identified. These challenges are largely systemic in nature, the result of existing structures and processes that can be improved.

Delivery Silos	Ministries work in silos, resourcing their own application development goals. This has presented obstacles to working in an integrated and collaborative manner. Numerous applications are duplicated in the province's data centres. These applications could essentially be reused. Staff across different ministries would benefit from forums to exchange lessons learned and solutions to common challenges.
Technical Drift	Complex legacy systems have been created over long periods of time and are slow to adapt. These legacy systems serve as barriers to change by introducing risk, technical debt, and maintenance. The "drift" occurs when legacy systems fail to adapt to new modern systems.
Service Model Gap	Out of date since 2009, the current service model was created to conform to the needs of most ministries at the time. Today, the shared service model is inflexible in meeting timely solutions. Ministries are consistently asking for a modernized application infrastructure approach, one that is underpinned by continuous improvement. In turn, this would free up ministry resources to focus on core operations.
Pit of Costs	The current delivery model is too expensive and lacks transparency. Cross-subsidization of services makes it challenging to evaluate and compare services on cost. We need more data to understand exactly how much we are paying for the delivery model and in turn enable informed decision-making.
Contract Challenges	Procurement processes have presented barriers to innovation. Contracts are often inflexible and do not consider changes, new products and services, nor reuse across government.
Unsustainable Application Growth	Often ministries address business needs by developing new custom applications, but they do not decommission old applications. Both systems require ongoing support, adding risk, extra resources, and cost. This reduces the ability for ministries to continuously improve their service offerings.
Losing the Security Marathon	Government is the custodian of people's data. This requires upholding security obligations and adhering to industry best practices. Government must develop new processes to continuously evolve and address emerging security risks.

Future state

We have also identified the corresponding opportunities associated with our challenges, which provide a sense of what good would look like at the enterprise or from the whole-of-government perspective. This is where we are going.

Working Better Together	By sharing knowledge and experience, including what works well and what does not, ministries can raise the overall maturity of their service delivery. Open communities and cross-functional teams, working across silos, will support broader engagement and increased client satisfaction.
Technical Diligence	Government can improve its service delivery by taking a more holistic approach to how it builds and buys information systems. This includes engaging with users early and often, establishing/using sound architectural standards, and leveraging best-in-class solutions.
Service Model Fit	There is an opportunity to increase value to stakeholders by reducing red tape, promoting self-serve where appropriate, and increasing transparency. Modern tools and services will provide a better experience for citizens and public servants alike.
Cost Optimization	Individual procurements can be better informed by increasing the transparency of fees for service across ministries. This will also lead to cost optimization through rationalization and aggregation of demand, as well as increased competition among vendors, which will drive costs down.
Collaboration over Contract Negotiation	A collaborative approach to vendor management will reduce duplication of effort for ministries and vendors alike. Contracting with multiple providers will better allow transition of services when desirable.
Sustainable Application Portfolio	Custom software applications come with a cost, not only for up-front development but also in long-term maintenance. By leveraging commodity services for common requirements, ministries can focus on what is unique in their mandate. This will also lead to an overall decrease in the number of systems across government, with corresponding reduction in maintenance efforts.
Keeping Pace in the Security Race	Configured appropriately, commercial, open source, and/or cloud-based services are more secure than bespoke solutions. Government has an opportunity to benefit from vendors' often sizeable security budgets, retiring legacy systems with security vulnerabilities, and embedding security in new applications.

Framework principles

Based on the current-state challenges and future-state opportunities, we have built a set of three key principles which provide guidance on how government moves forward:

1. **Strengthen technical capabilities, at the centre and in the ministries**
   Government will: support empowered, distributed communities of technologists; automate IT provisioning through routinized, scriptable and repeatable processes; and formalize and adopt robust architectural standards.

2. **Avoid being "too big to fail"**
   Government will: more effectively leverage procurements across government; prioritize independent professional services that add the greatest value; effectively orchestrate hosting services to maximize network performance and data portability; and act as an informed consumer of increasingly sophisticated hosting services.

3. **Adopt fit-for-purpose solutions and internet-era approaches**
   Government will collaborate with partners and vendors to maximize the return on investment by: adopting the highest-level services that meet business needs, including by minimizing unnecessary customization; adopting best practices in software development when custom application development is necessary; and convening integrated, cross-functional teams in developing applications.

These are further described below.

Strengthen technical capabilities, at the centre and in the ministries

To be successful, we need to strengthen our capability to deliver digitally within the OCIO.
But, that alone is not sufficient. We also need to ensure that capacity and capability is embedded in the ministries.

To strengthen technical capabilities, we will:

- champion governed, empowered communities;
- promote automation;
- endorse architectural standards; and
- ensure that privacy and security is everyone's responsibility.

Governed, empowered communities

The many are wiser than the few. The government is committed to fostering a community approach to innovation. This means providing direction, support, and guardrails for adoption of the Digital Framework.

We are committed to collaboration, knowledge sharing, and working in the open. This includes empowering people to adopt and master new technologies and leverage common components. These technologies will be compliant, best in class, and rapidly solve business problems. This approach will also enable evidence-based decision making and promote transparency.

Automation

Automation is the future. It allows government to develop and migrate IT infrastructure by avoiding the expense of manual effort. When repetitive and mundane tasks are automated, employee time is freed up to focus on other business priorities and technology needs. In addition, IT infrastructure can be automated by representing it as code using open source tools. This informs architecture choices and improvements and in turn, reduces our overall cost.

Along with IT infrastructure automation, reusable assets, known as common components, make it easier to deliver solutions that incorporate common business functionality. Examples include identity, payment, and integration in support of data exchange. Automation should include the ability to ensure performance through service measurement and analytics.

To support automation, ministries should adopt Agile and DevOps cultures, including site reliability engineering, along with cloud-native architecture, which foster frequent deployments, ensure high application availability, and support continuous improvement.

Architectural standards

The Government of British Columbia has adopted nine Architectural Principles. These principles establish architectural best practices and priorities and should be widely adopted and strengthened across the public sector. These principles will guide future architectural standards. The principles are further described in an appendix to this strategy.

The architectural principles include:

1. Love Thy User – co-design with consumers and a cross-functional team
2. Consider Common Value – re-use data, processes, services, technology, expertise
3. Authoritative Data – leverage an acknowledged source of truth
4. Make it Appropriately Secure and Private – use classification and common services
5. Build in Self-Improvement – facilitate ongoing user feedback, leverage analytics
6. Leverage Open – open source and standards for transparency, collaboration, and trust
7. Make it Interoperable – design for change and adaptability
8. Self-Serve Simplicity – products and components are easy to find and consume
9. Be Elastic – processes and technology can scale as needed

Privacy and security

These architectural principles are closely aligned with government's security principles. Security is everyone's responsibility. It is essential for employees, at every level, to understand the role that they play in protecting information and the many types of devices we use. Ministries must ensure that everyone in their organization understands the importance of security and its role in enabling the business to deliver.

The five security principles are:

- Risk Management
- Secure Patterns
- Security by Design
- Defence in Depth
- Data Protection

Risk Management

- Risk is related to the confidentiality, integrity, and availability of the information processed, stored, and transmitted by the system.
- Risk management is a business function; application security is a function of both development and operations. When analyzing application development and deployment risks, the organization's risk tolerance must inform acceptance, avoidance, or transference of each risk.

Secure Patterns

- Following vetted and approved patterns for security enables a consistent security posture and creates efficiencies in security efforts.
- Corporately produced and vetted, hardened system images should be used in lieu of bespoke purpose-built images wherever possible.
- Strong authentication components/libraries/patterns should be produced for corporate use and then consistently used across projects. Two-factor authentication should be available to all projects.
- Secure code patterns should be developed and available to all projects.
- Secure data transfer mechanisms should be available to all projects.
- Zero Trust mechanisms should be conscientiously deployed between all network components of an application.

Security by Design

- Security is always the foremost non-functional requirement of every application.
- Security consulting is provided by every Ministry's Information Security Officer as well as within the Exchange Lab.
- Application security enables compliance with FOIPPA privacy legislation.
- The security lifecycle of an application starts with security in the design, continues with secure coding testing, includes network security, and always requires patching and upgrading of components while in operation.
- Automated security testing needs to be built into the development process.

Defence in Depth

- Similar to the Defence in Depth concepts in IT infrastructure security, Defence in Depth in an application informs application and data architecture decisions.

- Separation of Duties, as a part of Defence in Depth, implies that functional components need to be focused on specific processes, as in a typical n-tier architecture.
- Least Privilege, as part of Defence in Depth within the application, implies that functional components should be isolated from each other. For example, high-privilege functions should be constrained, single, simple functions, as opposed to having access to everything.
- Least Privilege at the architectural level constrains functionality to only the necessary access to data where appropriate. For example, a read-only application programming interface (API) function should not have the ability to write data.
- Least Privilege at the business process level requires understanding who needs access to what data, when, and from where. Careful monitoring can uncover use of compromised credentials.

Data Protection

- Know your data to protect your data.
- The ministry should classify the data used in an application in alignment with the B.C. government's Information Security Classification Standard.
- The business area should understand who should have access to what data.
- Understand where the data is stored and processed, especially in light of FOIPPA constraints.
- Where appropriate, use encryption of data in transit, at rest, and during processing.

Avoid being "too big to fail"

Too often, things are grouped together for convenience sake at the time. This often has long-term, less-than-ideal consequences. The act of decoupling establishes boundaries that promotes modularity and reuse. This, in turn, leads to smaller, single-purpose components, faster delivery times, and the ability to more easily evolve as new approaches appear in more specific areas of concern.

Examples of decoupling include:

- Procuring once, using often;
- Receiving independent professional advice;
- Adopting hybrid cloud, hyper networks, and managed data;
- Securing best-in-class service.

Regularly products and services are procured solely on behalf of one ministry and are not readily reusable. We must procure commodity services so they can be reused going forward, regardless of lead ministry. New procurement processes should leverage flexible licensing and lower the total cost of ownership through shared agreements. They should grant more flexibility for ministries to consume and reduce vendor lock-in by negotiating shorter contracts.

Receiving independent professional advice means trusting our vendors but verifying their recommendations. It means adhering to the principles of fair and open procurement, supporting competition, ensuring value for money, and promoting transparency and accountability. We must avoid situations where advice may be biased due to other interests of the professional services firm.

Cloud has increasingly become the new industry standard for how technology is delivered to support digital service delivery. Cloud computing provides a commodity service for government, supported by an ever-expanding marketplace. This increases the agility, flexibility and speed of delivery for digital services. It removes the big, up-front investments in technology to enable scaling up or down quickly. This provides much-needed flexibility and the ability to respond to changing demands. It has the potential to enhance collaboration, limiting the duplication of solutions and reducing the amount of maintenance effort required to "keep the lights on." This allows ministries to refocus that effort.

As we decouple, government must ensure that data is portable. Solutions should be designed for cloud mobility and include an exit strategy to prevent vendor lock-in.

Government needs to become a better-educated consumer, seeking out best-in-class services that:

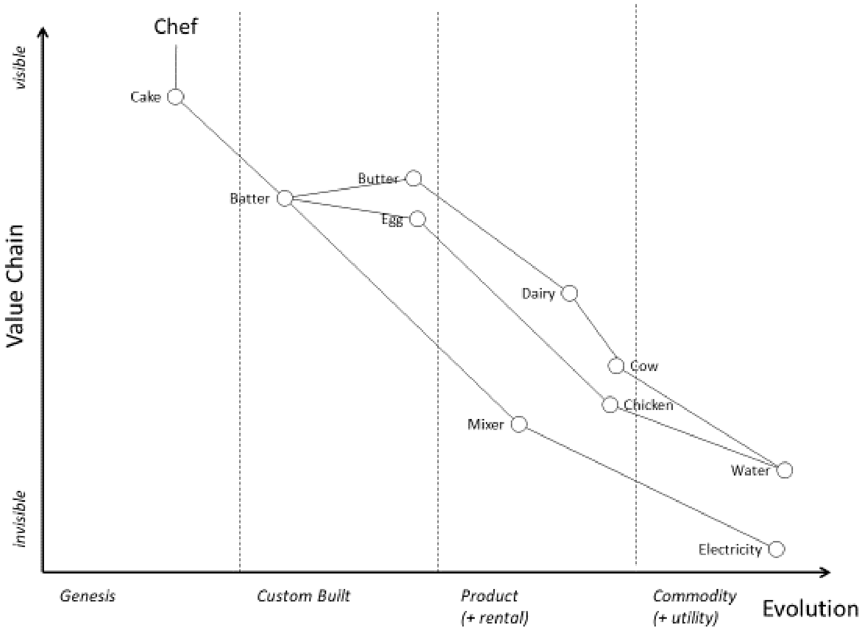
- Meet legal and regulatory compliance and provide resilience from security threats;
- Enable ministries to grow, maintain, and modernize solutions that meet their business needs;
- Are supportable by vendors and/or community;
- Incentivize a shift towards common components and reduce risk and technical debt;
- Are accessible, not device dependent;
- Enable data sharing between ministries; and
- Are cost effective.

Adopt fit-for-purpose solutions and internet-era approaches

To better deliver services, government needs to appropriately balance custom versus bespoke solutions. Solutions are typically created through the orchestration of three main building blocks or components: software, compute, and storage. Internet-era approaches involve each of these categories.

One of the models to illustrate commodity versus custom building blocks is a Wardley map. In a Wardley map, the components of an overall solution are classified according to the perceptible value they provide to a stakeholder and the ubiquity or commodity of the components themselves.

For example, to bake a custom-order cake, a chef needs several ingredients and tools. The cake itself is unique, tailored to the request of the consumer. To make the cake, the chef requires butter and eggs from grass-fed cows and free-range chickens. The chef does not know or care which cows and chickens provided the milk and eggs. The cows and chickens require water. The water is even further removed, in terms of visibility, from the chef. The water may come from the municipality, or from a well, or it might be trucked in. In this example, the water quality is the same regardless of source.



It does not make sense for the chef to keep his own livestock, or to run his own hydroelectric or water utilities. These are commodity services, available from multiple sources with little differentiation.

The same model, applied to government IT, means consuming best-in-class, readily available services rather than building them from scratch. It means leveraging work that has already been completed, including common components. In turn, this frees up resources to shift left and add value where it counts. Ministries can focus on their core competency, which is service delivery within their sector, through the use of commercial and/or open source tools. Conversely, ministries can provide valuable feedback and knowledge to the vendor community regarding the problems they are trying to solve. This notion of open innovation represents the inflows and outflows of ideas, leading to better service delivery for British Columbians.

When we do need to build, we bring in the newest tools and approaches to maximize effectiveness, efficiency and sustainability. This leads to an increase in visible value for stakeholders.

We have an opportunity to free up IT staff time by managing as little IT infrastructure as possible. Moving up the stack means acquiring capabilities that allow the business to deliver on the needs of the end user.

This will allow government to more readily refactor or retire legacy systems to take advantage of the rise of utility services. We move up the stack from consuming infrastructure to consuming as-a-service offerings. This means software-as-a-service (SaaS) and low-code/no-code platforms are preferred over custom development, where the available service offerings are a good fit. How do we determine if a particular offering is a good fit? This is the purpose of solution architecture and guidance will be cocreated with the community, working in the open, to help drive a consistent approach aligned to this strategy and tied to our architectural principles.

When we must develop something net-new and custom, it should be developed using best-in-class approaches. This means:

- Ensuring that development, security, and operations (DevSecOps) teams work collaboratively;
- Adopting newer architectures and approaches that enable organizations to “shift left”; and
- Focusing on continuous delivery and quality assurance.

Cross-functional delivery teams should be empowered to innovate and leverage new solutions. Such teams integrate key units, including business, privacy, security, IT, design, management, front line, end users, procurement, and legal.

Notice of direction

The principles, current-state challenges and future-state opportunities provide our notice of direction and provide guidance on the direction of IT service delivery in the B.C. government. Further development of related policies and standards will include alignment with government principles and policies and input from the MCIO Reference Group, Technology Innovation Forum, as well as the public.

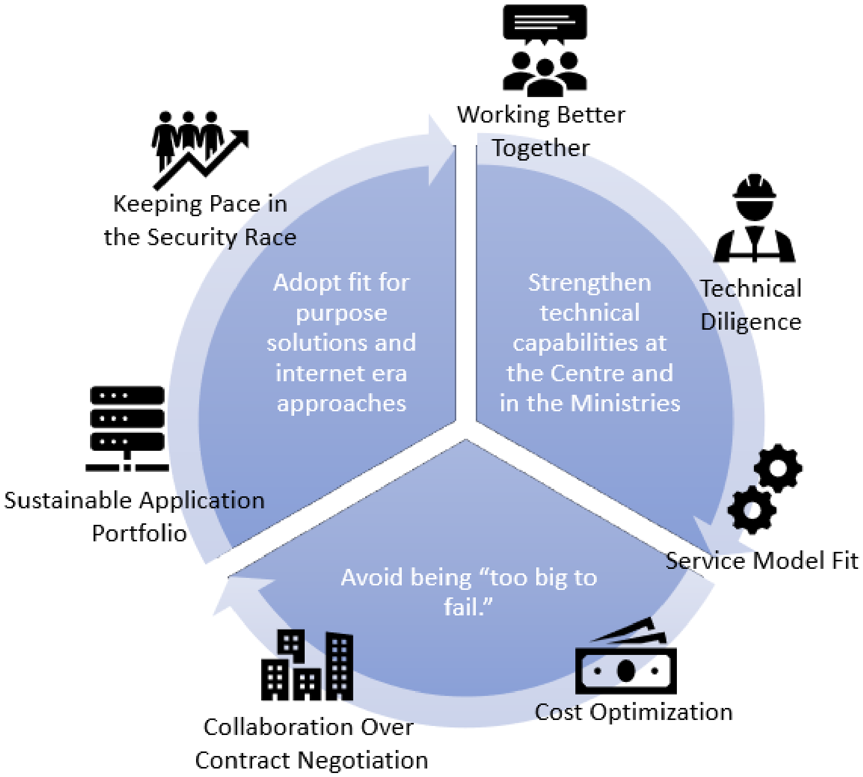
The following table outlines our current and future state and how we get there using a principles-based approach.

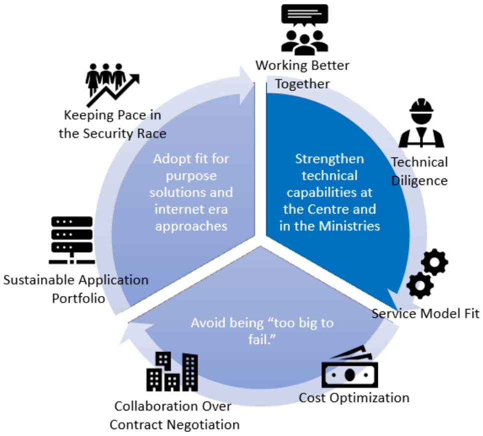
From (current state)	To (future state)
Delivery Silos Ministries work in siloes, resourcing their own application development goals; they often fail to work in an integrated and collaborative manner.	**Working Better Together** Open communities, working cross government, sharing lessons learned beyond project teams.
Technical Drift A proliferation of complex legacy systems has been created over time; these systems are slow to adapt and introduce risk and technical debt requiring costly care and feeding.	**Technical Diligence** Improved technical hygiene from IM/IT solutioning to software engineering – working in the open.
Service Model Gap The current IM/IT service delivery model is inflexible; it was created to conform to the needs of most ministries but is constrained in supporting timely solutions.	**Service Model Fit** Self-serve, modern experience with transparent services, costs and communities.
Pit of Costs Current delivery model is perceived to be too expensive; the cost model is opaque and the cross-subsidization of services makes it challenging to evaluate services on cost.	**Cost Optimization** Transparent fees for services, competitive offerings drive cost optimization across the eco-system.
Contract Challenges Contracts are often inflexible and do not adapt to change, support new services or facilitate reuse across government.	**Collaboration over Contract Negotiation** Smaller more numerous agreements allowing for best-in-class services and service transition.
Unsustainable Application Growth Ministries address business needs by developing new custom applications; old apps are not decommissioned, and ongoing support is required, adding risk, extra resource needs and costs	**Sustainable Application Portfolio** Fewer custom applications more SaaS, fewer lower-level services requiring self management.
Losing the Security Marathon Government is the custodian of people's data; it must uphold security obligations and adhere to continuously evolving industry best practices.	**Keeping Pace in the Security Race** Benefiting from service providers' larger security budgets, retiring legacy debt and embedding security.

4. How we will get there

The "Where we are going" section and specifically in the "Principles" and "Notice of direction" sections share tangible examples of what needs to be done to drive improvements in IT service delivery across government. There is no single, defining action to achieve these improvements, but rather a series of small actions, which, together, will yield success. The process is like moving a heavy flywheel, resistant at first but gaining momentum with each turn. We have adopted this flywheel construct to illustrate that:

1) all these efforts work together creating momentum and progress towards our goal; and
2) this will be an ongoing journey of continuous improvement and adaptation.


Working Better Together
Keeping Pace in the Security Race
Technical Diligence
Adopt fit for purpose solutions and internet era approaches
Strengthen technical capabilities at the Centre and in the Ministries
Sustainable Application Portfolio
Service Model Fit
Avoid being "too big to fail."
Cost Optimization
Collaboration Over Contract Negotiation


Working Better Together
Technical Diligence
Service Model Fit
Cost Optimization
Collaboration Over Contract Negotiation
Sustainable Application Portfolio
Keeping Pace in the Security Race
Strengthen technical capabilities at the Centre and in the Ministries
Adopt fit for purpose solutions and internet era approaches
Avoid being "too big to fail."

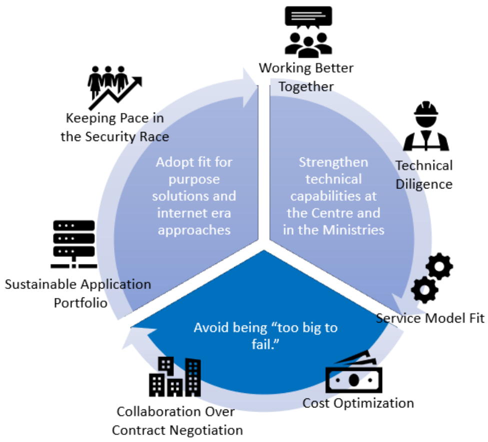
Strengthen technical capabilities, at the centre and in the ministries

Government will: support empowered, distributed communities of technologists; automate IT provisioning through routinized, scriptable and repeatable processes; and formalize and adopt robust architectural standards.

Our Next Steps: Goals	Our Measures of Success
Create instant provisioning of government compute environments[1]	Create curated catalogue of cloud technical capabilities Create enterprise solution for provisioning processes for majority of compute, network, and storage
Empower stakeholders with knowledge-sharing tools, and processes and encourage them to work in the open	Create in-the-open playbook for Customer Relationship Management Create application playbook Create registry playbook
Formally adopt the proposed Architecture Principles (as referenced within this strategy) through a formal policy instrument (e.g., a GCIO policy directive)	Review with Architecture Standards Review Board and receive formal GCIO endorsement
Create a community of practice for technology innovation across government	Grow the Technology Innovation Forum to include an active and representative member from each ministry and/or sector, to promote better communication and knowledge sharing
Evangelize for integrated HR approaches to solution delivery	Write three cases studies on multidisciplinary teams leading to success Continue to review funding requests to ensure cross-functionality teams are intended[2]

[1] Led by Cloud Pathfinder and Enterprise Services

[2] Led by Tech Review Team


Working Better Together
Keeping Pace in the Security Race
Technical Diligence
Adopt fit for purpose solutions and internet era approaches
Strengthen technical capabilities at the Centre and in the Ministries
Sustainable Application Portfolio
Service Model Fit
Avoid being "too big to fail."
Collaboration Over Contract Negotiation
Cost Optimization

Avoid being "too big to fail"

Government will: more effectively leverage procurements across government; prioritize independent professional services that add the greatest value; effectively orchestrate hosting services to maximize network performance and data portability; and act as an informed consumer of increasingly sophisticated hosting services.

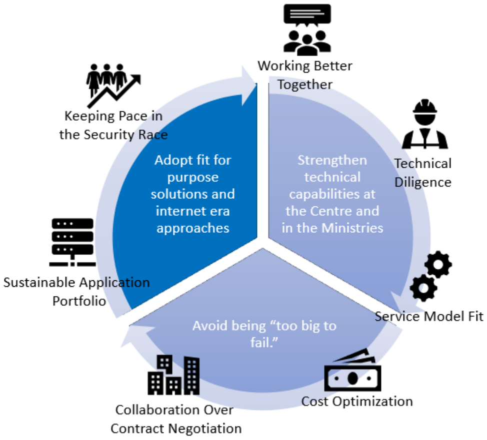
Our Next Steps: Goals	Our Measures of Success
Roll out new Enterprise Services funding model, removing cross subsidization of services[3]	Seek approval to realign delivery costs with fee levels at the service level
Facilitate changes to procurement practices to enable greater reuse of ministry SaaS procurements	As part of overall efforts to catalog government IM/IT, support development of central repository to track SaaS procurements across government Develop a playbook to support reuse of pre-existing contracts Initiate changes to General Service Agreements (GSAs) to support sharing and reuse by default
Support identity and access management strategy for hybrid cloud[4]	Establish corporate privileged identity management (PIM) and privileged access management (PAM) Enable access control based on roles for users and administrators in a multi-cloud environment
Increase adoption of the Object Storage service as a storage methodology for government data[5]	Support movement of 5% of government data to the Object Store, increasing by 5-10% per year thereafter until 50% of government data is stored using this service
Re-architect the Shared File solution[6] to reduce cost to government and client organizations	Reduce capital and operating costs of the Shared File service

[3] Led by Enterprise Services funding model review

[4] Led by Cloud Pathfinder and Information Security Branch

[5] Led by Enterprise Services shared file/print project

[6] Also led by Enterprise Services. Shared File is government's centralized approach to network file storage and management


Working Better Together
Technical Diligence
Strengthen technical capabilities at the Centre and in the Ministries
Service Model Fit
Cost Optimization
Avoid being "too big to fail."
Collaboration Over Contract Negotiation
Sustainable Application Portfolio
Adopt fit for purpose solutions and internet era approaches
Keeping Pace in the Security Race

Adopt fit for purpose solutions and internet era approaches

Government will collaborate with partners and vendors to maximize the return on investment by: adopting the highest-level services that meet business needs, including by minimizing unnecessary customization; adopting best practices in software development when custom application development is necessary; and convening integrated, cross-functional teams in developing applications.

Our Next Steps: Goals	Our Measures of Success
Establish additional SaaS/ platform-as-a-service (PaaS) agreements for corporate use	Identify candidate SaaS/PaaS offerings and establish umbrella agreement for reuse by ministries
Baseline application count, begin tracking the decommissioning of legacy applications corporately Baseline number of legacy applications on extended warranty status, track corporately	Following the completion of application portfolio summary and to be determined with MCIOs, targeting a downward trend
Include modern and self-serve security services, including vulnerability scans, code reviews, etc.	Enable clients to self-provision services such as vulnerability scans for web-based applications

Next Steps

The Framework's impact will help close the service expectation gap and continue to enhance security and protect privacy.

There are three streams of work:

- a common understanding of the current state of government's IT landscape
- a vision for the future state
- tactics to help us get there

The next steps are outlined below as deliverables B through E.

Deliverable B: Application Portfolio Summary

- The summary will outline the current state of government's 1,600+ applications
- What can be summarized about the current portfolio
- Costs to develop, host, and maintain the current portfolio
- The number of custom-built vs commercial off-the-shelf and SaaS
- The average amount of time since the last minor and major releases of the custom-built applications
- Specific types or classes of applications

Deliverable C: Playbook for Modern Application Architecture

- The playbook will provide guidance on adoption strategies, efficiencies, and implementation.
- Adoption strategies – 6Rs (rehost, replatform, repurchase, refactor, retire, and retain)
- Lessons learned and key success factors
- Analysis of 6Rs against common application archetypes
- Resources (e.g., standards, other supports in government)
- Cost analysis guidance

Deliverable D: Future State Blueprint

- The blueprint will propose a reference architecture and measurable use cases delivering high business impact. The Common Components Program Framework is also connected to this work
- Assess capabilities the government owns today
- Assist in identifying leading technologies as part of a portfolio of common components
- Support alignment between business units
- Present best practices from leading government
- Inform interfaces between legacy and new systems
- Completion: to be determined, dependent on technical architect resourcing, community participation, and executive governance

Deliverable E: Policy Instruments

The Framework will be influenced by numerous policies and principles including:

- The Digital Policy Framework
- CPPM Chapter 12 (being updated)
- Managing Government Information Policy (in development)
- Appropriate Use Policy (being updated)
- Information Security Policy and Guidelines
- CPPM Chapter 6, Procurement (in development)
- Standards of Conduct
- Various technical and security standards administered by the OCIO (over 40+ standards)
- Principles informing the Framework including:
  - Digital Principles
  - Ten Principles of Privacy Protection
  - Procurement Principles
  - OCIO Architectural Principles
- Completion: to be determined, dependent on technical architect resourcing, community participation, and executive governance

Appendix - ***OCIO Architectural Principles***

OCIO Architectural Principles (Jan 2020)
Love Thy User – co-design with consumers and a cross-functional team
• Artifacts that demonstrate user engagement (e.g., journey maps, user stories, personas, screen mockups, demographic, geographic, ethnographic) • Recognition of different stakeholder communities, their diverse interactions, practices, communication styles, devices, and accessibility requirements. Test with these users • Take measurements that are actionable, analyze the data, and act on it • Establish methodologies and opportunities for regular facilitated feedback, and for unsolicited feedback from users • Adheres to own published service standards (e.g., system uptime, system response times, help desk response times)
Consider Common Value – reuse data, processes, services, technology, expertise
• Reuse before re-creating (e.g., B.C. Data Catalogue, design system, SaaS) • Design solutions that are scalable across government • Is consumable as a common component • Consumes common components
Authoritative Data – leverage an acknowledged source of truth
• System of record identified • Plan to integrate to the source of truth • Consume authoritative data as a microservice • Expose authoritative data as a microservice
Make It Appropriately Secure and Private – use classification and common services
• Privacy impact assessments and security threat and risk assessments • Use the appropriate collection and storage for data • If user identification required, comply with an acceptable provincial identity standard • Source code is scanned for vulnerabilities • Appropriate level of vulnerability scanning and penetration testing • Privileged user back-end access is monitored
Build in Self-Improvement – facilitate ongoing user feedback, leverage analytics
• Define and describe a minimum viable product • Iterate and improve frequently to support learning, innovation, and continuous improvement • Facilitate continuous consumer feedback to the product team's roadmap • Leverage analytics to support feature prioritization • Monitor product health and performance • Automate as much as possible, e.g., testing, documentation, deployment, and measurement
Leverage Open – open source and standards for transparency, collaboration, and trust
• A shared repository holds the code • Leverage open source • Leverage open standards (including data standards) • Avoid vendor lock-in

OCIO Architectural Principles (Jan 2020)
• Healthy community working in the open, co-creating, and collaborating
Make it Interoperable – design for change and adaptability
• Design is modular, plug and play • Register your component, making it easy to find and use • Design documents that illustrate what the product does • Plan for data portability • Microservices are the component of choice
Self-serve Simplicity – products and components are easy to find and consume
• The product consists of a suitably small set of APIs • Consumption is platform-agnostic • Implementation in a very short timeframe and cost effective • Consumer reviews attest to favorable, self-serve implementation
Be Elastic – processes and technology scale as needed
• Design for scalability • Consumption cycles are predicted • Implement business process that accommodates peak and low use • The platform can accommodate spikes, optimizing costs and resources • Technical adjustments are automated • Follow modern software development methodologies (e.g., The Twelve-Factor App)